AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH TWO GOOGLE ACCOUNTS THAT ARE STORED AT PREMISES CONTROLLED BY GOOGLE LLC

Case No. 1:22-mj- 670-DJS

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1470, 2422(b), 2251(a), 2252A(a)(2), 2252A (a)(5)	Transfer of Obscene Material to a Minor, Coercion and Enticement of a Minor, Production of Child Pornography/Sexual Exploitation of Children, Receipt of Child Pornography, Possession of Child Pornography

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Rebecca Gworek

Applicant's signature

Rebecca Gworek, FBI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: 11/2/2022

Judge's signature

City and state: Albany, NY

Hon. Daniel J. Stewart, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH TWO GOOGLE ACCOUNTS THAT ARE STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 1:22-mj- 670-DJS Filed Under Seal

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANT

I, **Rebecca Gworek**, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a warrant to search information associated with two accounts (each a "Target Account") that are stored at premises owned, maintained, controlled, or operated by Google LLC ("Google" or "Provider"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(l)(A), and 2703(c)(l)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am an investigator with the Federal Bureau of Investigation (FBI) and have been since January 2016. I am assigned full-time to the Albany Division, Albany, N.Y. I have investigated a variety of violent crimes including violent gangs, domestic terrorism, child sexual exploitation, and assault. My current duties include investigating criminal violations relating to child exploitation and child pornography, including enticement and coercion of minors, as well as

production, distribution, receipt, and possession of child pornography. I have gained experience regarding such crimes through training in seminars, classes, and everyday work in those types of investigations. My investigative experience includes interviewing victims and witnesses, as well as conducting searches of physical locations, email accounts, social media, and electronic devices, as well as use of location information to identify and locate criminals.

3. I have also received training in the area of Child Sexual Abuse Material (CSAM) and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, and I am authorized by law to request a search warrant.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Where statements of others are related in this affidavit, they are related in substance and in part.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2422(b) [Coercion and Enticement of a Minor], 2251(a) [Production of Child Pornography], 2252A(a)(2) [Receipt of Child Pornography], 2252A(a)(5) [Possession of Child Pornography], and 1470 [Transfer of Obscene Material to a Minor] (the "Subject Offenses") have been committed by Isaiah Lafoe. There is probable cause to search each of the Target Accounts, further described in Attachment A, for evidence and instrumentalities of these crimes, as further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. § 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. The United States, including the FBI, is conducting a criminal investigation of ISAIAH LAFOE for potential violations of the Subject Offenses. Between December 2020 and March 2021, Lafoe, aged 22 years old at the time, communicated with a then-13-year-old girl ("Victim-1") via social media, including Google Duo, and by phone, and Victim-1 sent Lafoe sexually explicit nude images and videos of herself. A 13-year-old boy in Reno, Nevada ("Victim-2") reportedly also communicated with LaFoe in the summer of 2021. Based on the FBI's investigation, Lafoe owns, controls, and used **Target Account lafoeisaiah28@gmail.com** to communicate with Victim-1, who owns or controls the **Target Account miltonwilliamsaiesha@gmail.com**.

Victim-1

8. In late February 2021, a 13-year-old girl (Victim-1) and her mother, both residents of Troy, New York, reported to the Troy Police Department (TPD) that Victim-1 had been coerced into sending sexually explicit images to an adult male. During interviews with law enforcement, including TPD, and later the FBI, Victim-1 reported that:

a. In late 2020, Victim-1 discovered an online website, Omegle.[1] Using Omegle, Victim-1 met one individual, later identified as Lafoe, and then befriended and

[1] Omegle is a free online chat website that allows users to socialize with others by randomly pairing users in one-on-one chat sessions where they chat anonymously.

messaged him on another social media application, Snapchat.[2] According to Victim-1, Lafoe also communicated with her via phone (including FaceTime), Google Duo,[3] as well as other video messaging applications such as the social media application, TikTok.[4]

b. According to Victim-1, when she initially met Lafoe online, he presented himself as being 15 but later informed Victim-1 that he was 19. Victim-1 also informed law enforcement that she told Lafoe that she was 13 years old. Lafoe informed Victim-1 that he wanted to meet her, but they had to wait until Victim-1 was 18 years old.

c. According to Victim-1, Lafoe told her his name was "Isaiah Lafoe." During the conversations, Lafoe told Victim-1 that he resided in New Hampshire at an undisclosed address.

d. Victim-1 also provided a description of Lafoe matching the description known to law enforcement for Lafoe by describing Lafoe as a white male with facial hair and a tattoo on his left arm with his grandmother's name. An image was shown to Victim-1 of LaFoe, which Victim-1 positively identified as Lafoe and was the same male she had been video chatting, texting, and communicating with and was the same male who had asked her for and that she sent sexually explicit and lascivious images.[5]

---

[2] Snapchat is an instant messaging app and service owned and controlled by Snap, Inc. that permits users to send and receive pictures, videos, and messages are usually only available for a short time before they become inaccessible to their recipients.

[3] Google Duo is a voice over IP (VoIP) and videotelephony service developed by Google LLC that lets users make and receive one-to-one and group audio and video calls with other users and can be used either with a phone number or an email account, allowing users to call someone from their contact list.

[4] TikTok is an instant messaging app and short-form video hosting service that permits users to send and receive pictures, videos, and messages.

[5] The image shown to Victim-1 is available for the Court's review upon request.

e. When asked about the images she created and sent to Lafoe, Victim-1 reported that Lafoe "roped" her into making the images and promised not to show anyone else. Initially, Victim-1 sent images of herself in outfits, and then later, sent images of her breasts and vagina. Victim-1 started with still photographs and then transitioned to videos. The videos were made with her phone and sent via Snapchat and TikTok.

f. When asked about the progression of the production of the videos, Victim-1 reported that Lafoe asked for more and more photos and that over time she trusted him. Victim-1 reported that some of the videos depicted Victim-1 masturbating and doing whatever made Lafoe feel good. Victim-1 also confirmed that she had used an object in her vagina to masturbate and sent the video to Lafoe. Victim-1 reported feeling disgusted after making the videos.

g. Victim-1 told Lafoe she lived in Albany, New York during their communications and her location was visible in her online profiles as being in Troy, New York. Victim-1 reported that all the videos and images she created for Lafoe were produced in Troy, New York at her house.

h. Victim-1 reported that she communicated with Lafoe via phone, and he was using phone number XXX-XXX-2010 (the "Target Phone -2010").[6] She also reported that the Google account she used to communicate with Lafoe was **miltonwilliamsaiesha@gmail.com** (a **Target Account**).

9. Victim-1 and her mother consented to the search of Victim-1's phone, which was subsequently extracted and reviewed by law enforcement and found to contain child pornography

[6] Records from Verizon Wireless show that the Target Phone -2010 has a listed subscriber with an address in Lancaster, New Hampshire.

of Victim-1. Metadata associated with the images confirm that the child pornography images and videos were taken with the same make and model device as Victim-1's phone, an LG model LM-X320PM smartphone, manufactured in China. Victim-1 stated all the child pornography images and videos on her phone were produced at Lafoe's request and sent to him via Snapchat, TikTok, or other social media application. Below are descriptions of one image and three videos, among others, found in the files on Victim-1's phone, all of which are available for the Court's review upon request:

a. An image with file name IMG-20201027-WA0008.jpg depicting a close-up of Victim-1 with her legs spread and the focal point as Victim-1's vagina. The metadata associated with the video file shows that it was created on or about October 27, 2020.

b. A video with MD5 hash value 7007584d771f2216e2b416c64a61e735, lasting 9 seconds, depicting Victim-1 with her legs spread and the focal point as Victim-1's vagina, and showing Victim-1 inserting her fingers into her vagina to masturbate. The metadata associated with the video file shows that it was created on or about October 5, 2020, and has a file path associated with Snapchat.

c. A video with file name 1605005528172.mp4, lasting 58 seconds, depicting Victim-1 with her legs spread and the focal point as Victim-1's vagina, and showing Victim-1 inserting the handle of hairbrush into her vagina to masturbate. The metadata associated with the video file shows that it was created on or about November 21, 2020.

d. A video with file name 1613008418365.mp4, lasting 13 seconds, depicting Victim-1 with her legs spread and the focal point as Victim-1's vagina, and showing

Victim-1 inserting an object into her vagina to masturbate. The metadata associated with the video file shows that it was created on or about February 10, 2021.

10. The extracted data from Victim-1's phone also showed that the phone contained 18 installed applications, including Omegle, Snapchat, TikTok, and Google Duo; a contact name "My Bff" with username "i_lafoe20," which was added on September 30, 2020; and a contact name "BD" associated with the phone's numbers XXX-XXX-3620 ("Target Phone -3620"), and the Target Phone -2010. Victim-1's phone also had at least three images showing a split-screen screenshot of a video chat message, including an image matching the description of Lafoe on the left and an image of Victim-1 standing nude and pouring an unknown white liquid onto her chest. The image's metadata shows that the image was created on or about November 15, 2020.

11. Victim-1's phone also contained several video files of Lafoe, including a video file with file name 2fde823d-1437-4873-a2a5-11fb74eecbc3.mp4 showing Lafoe's face and matching his description, laying nude on a bed, stating "Look at what you're missing pendeja"[7] and then showing Lafoe's penis and semen on Lafoe's on his chest and torso. The metadata associated with the above video file shows that it was created on or about November 8, 2020.

12. Victim-1's phone also contained electronic text communications between Victim-1 and Target Phone -7922, including the following text message exchange on September 30, 2020:

Sender	**Date**	**Message**
Victim-1	9/30/2020 2:11:57 AM(UTC-4)	I have something to tell you something
Victim-1	9/30/2020 2:15:59 AM(UTC-4)	Im 16 but i thought you was so hot and i lied so i can be with you
Target Phone -3620	9/30/2020 2:27:33 AM(UTC-4)	So you still can be with me
Victim-1	9/30/2020 2:29:09 AM(UTC-4)	Yes

[7] I understand that "pendeja" is a mildly vulgar insult for "asshole" or "idiot" in Spanish.

Sender	Date	Message
Target Phone - 3620	9/30/2020 2:29:34 AM(UTC-4)	Your mom said it's fine
Target Phone - 3620	9/30/2020 2:31:14 AM(UTC-4)	You going to wait till you turn 18 to say something
Target Phone - 3620	9/30/2020 2:32:16 AM(UTC-4)	So you not going to say nothing till you 18 and you a virgin
Target Phone - 3620	9/30/2020 2:34:29 AM(UTC-4)	When you lost your virginity
Target Phone - 3620	9/30/2020 3:02:30 AM(UTC-4)	Or I will fuck you so good and before I cum I will cum in your mouth
Target Phone - 3620	9/30/2020 3:03:48 AM(UTC-4)	You gonna swallow it too
Target Phone - 3620	9/30/2020 3:44:37 AM(UTC-4	Baby I said I have you to help me cum
Target Phone - 3620	9/30/2020 3:45:49 AM(UTC-4)	i_lafoe20

13. Victim-1's phone also contained electronic Snapchat communications between Victim-1 and Snapchat user "i_lafoe20,"[8] including a Snapchat message on September 30, 2020 with Snapchat user i_lafoe20 stating as follows:

Sender	Date & Time	Message
i_lafoe20	9/30/2020 3:52:26 AM (UTC-4)	Hey baby
Victim-1	9/30/2020 3:52:46 AM (UTC-4)	Hi daddy
i_lafoe20	9/30/2020 3:56:01 AM(UTC-4)	Baby send me a pussy pic
i_lafoe20	9/30/2020 3:58:40 AM(UTC-4)	Pop a tit and take a pic

14. Victim-1 also had the following correspondence with Snapchat user i_lafoe20 on October 5, 2020, which in my training and experience indicates that Lafoe received images and

[8] Snap, Inc. records show that a Snapchat account with username "i_lafoe20" was created on September 4, 2020, with display name "Isaiah Lafoe." A phone number XXX-XXX-7922 ("Target Phone -7922") was listed under the account and as of July 2022, the account remained active.

videos from Victim-1, which may have included the video depicting child pornography listed in Paragraph 7.b above that was created on or about October 5, 2020:

Sender	**Date & Time**	**Message**
Victim-1	10/5/2020 5:52:52 PM (UTC-4)	Bae i have something for you
Victim-1	10/5/2020 6:17:37 PM (UTC-4)	So u like wat i can do
i_lafoe20	10/5/2020 6:19:23 PM (UTC-4)	Hell yeah
Victim-1	10/5/2020 6:19:53 PM (UTC-4)	Will that all for you

15. Victim-1's phone also contained electronic text communications between Victim-1 and Target Phone -3620 on November 15, 2020:

Sender	**Date**	**Message**
Target Phone -3620	11/15/2020 7:17:09 PM (UTC-5)	Suck em tits real good
Target Phone -3620	11/15/2020 7:17:47 PM(UTC-5)	Do it or else
Target Phone -3620	11/15/2020 7:22:56 PM(UTC-5)	Suck em real good if you don't I will date your friend
Victim-1	11/15/2020 7:23:30 PM(UTC-5)	Ok daddy
Target Phone -3620	11/15/2020 7:25:20 PM(UTC-5)	Make your daddy proud and cum
Target Phone -3620	11/15/2020 7:27:26 PM(UTC-5)	Now fuck yourself

16. Call records from Victim-1's phone also show 12 calls between Victim-1's phone and Target Phone -2010 between December 12, 2020, and February 15, 2021.

Online Activity of Lafoe

17. Records from Microsoft Corporation, dated May 3, 2021, show that a Microsoft account was registered to "Isaiah Lafoe" (the "Lafoe Microsoft Account"), and listed an email address of **lafoeisaiah28@gmail.com** (a **Target Account**). The Lafoe Microsoft Account was

associated with Xbox gaming activity, including IP activity under gamer tag "Havokofdis98" between February 11, 2021, to April 11, 2021, using IP address 67.253.52.0., which is associated with a subscriber at an address in Lancaster, New Hampshire.

18. Meta Platforms, Inc. records show that a Facebook account with vanity name isaiah.lafoe.16 was registered in the name of "Isaiah Lafoe" on October 20, 2020 and registered with **Target Account lafoeisaiah28@gmail.com**. The public profile information on the account shows a profile photograph matching the description for Isaiah Lafoe. The account user is linked to 699 friends, most of which appear to be female. On December 19, 2020, the account user posted a video showing Isaiah Lafoe petting a dog. On November 9, 2020, the account user updated the profile to show that the user was "In a Relationship" and then posted a message stating "[G.T.] baby that's me and you" and linking to G.T.'s profile. Based on my review of G.T.'s profile, it appears that G.T. may have been under the age of 18 at the time.

Victim-2

19. On or about July 28, 2021, a 13-year-old boy located in Reno, Nevada ("Victim-2"), through his mother, reported to NCMEC that he had been communicating with an individual named "Isaiah" at an unknown address in New Hampshire for the previous three months. Victim-2 reported that "Isaiah" had communicated with him using mobile phone number XXX-XXX-5558 ("Target Phone -5558"). Victim-2 reportedly met "Isaiah" while playing an online game called "Call of Duty."[9] According to Victim-2's mother, "Isaiah" had been grooming Victim-2 and turned him into a girl; the child was no longer acting like himself as a boy would and had been acting like his sisters around the house. "Isaiah" had reported called Victim-2 "bae" and "wifey"

[9] Based on public sources, Call of Duty is a first-person shooter video game franchise published by Activision that can be played using various computer, gaming, and mobile platforms, including on a smartphone and Xbox. See https://www.callofduty.com/

and told Victim-2 that they were engaged and that he was going to "come for him and marry him." Victim-2 and "Isaiah" video chatted on Google Duo and the social media application TikTok. Victim-2's mother reported that Victim-2 had exchanged photos with "Isaiah" but did not know if the child sent real photos of himself.

20. Records from Verizon Wireless show that Target Phone -5558 has a listed subscriber of "Isaiah Lafoe" with an address at the Subject Premises.

Undercover Activity

21. On October 29, 2021, an officer acting in an undercover capacity utilizing the persona of a thirteen-year-old male (the "UC") investigated the Microsoft Xbox gaming platform associated with gamertag "Havokodis98," which is linked to **Target Account lafoeisaiah28@gmail.com** as noted above. The UC sent a friend request to the user of Havokodis98, which was promptly accepted. The user of the Havokodis98 account replied with a message to the UC stating, "I can't hear you." The UC then utilized an audio capable headset and made voice contact with "Havokodis98." Through the conversation, the user of the Havokodis98 account stated that his name was "Isaiah," that he was 23 years old and stated that he was currently located in Concord, New Hampshire. "Havokodis98" provided his cellular telephone number as Target Phone -5558 and requested that the UC send him a text message. The user of Havokodis98 also provided his Facebook account name to the UC as "Izzy Ray."

22. On July 13, 2022, an officer acting in an undercover capacity further investigated the Xbox gaming platform associated with gamertag "Havokodis98." As of July 13, 2022, the Xbox account for gamertag "Havokodis98" was still active and the profile photo on the account matched available photographs and the description for Isaiah Lafoe.

The Target Account lafoeisaiah28@gmail.com

23. Records from Google LLC show that the **Target Account lafoeisaiah28@gmail.com** was registered in the name of "Isaiah Lafoe" on October 20, 2020. The **Target Account lafoeisaiah28@gmail.com** listed Target Phone -3620 as both a recovery SMS number and as a Sign-in Phone number and listed IP activity associated with 67.253.52.249. Other phone numbers used on the account included Target Phone -2010 and Target Phone -5558. The **Target Account lafoeisaiah28@gmail.com** utilizes the following Google services: Gmail, Web & App Activity, Location History, Google Keep, Google Calendar, Android, YouTube, Google Payments, Play Loyalty. As of when records were produced, the last logins on the account were on July 26, 2022. Google records also show that a Google Duo account ID was created on October 23, 2020, and was linked to Target Phone -3620.

24. Records from Google, produced pursuant to an 2703(d) order issued by this Court on August 18, 2022, also shows that between at least July 12, 2021, and August 10, 2022, **Target Account lafoeisaiah28@gmail.com** received emails from the following email addresses: callofduty@marketing.activision.com, callofduty@comms.activision.com, xbox@engage.xbox.com, no-reply@youtube.com, birthdays@facebookmail.com, notification@facebookmail.com, friendupdates@facebookmail.com, reminders@facebookmail.com, mentions@facebookmail.com, and friends@facebookmail.com. Based on the domains for these emails, I believe these emails were automated emails from Call of Duty, Activision, Xbox, YouTube, and Facebook, all of which were applications used by Lafoe.

25. Records from T-Mobile show that Target Phone -3620, was active and had made calls between December 25, 2020, and March 25, 2021.

26. Google IP records produced in response to an order authorizing the installation and use of a pen registered and trap and trace device for **Target Account lafoeisaiah28@gmail.com** shows that there was a login from IP address 67.253.52.249 on July 23, 2022.

27. Charter Communications records show that IP address 67.253.52.249 was registered to a subscriber with initials T.D. with a listed address on Portland Street in Lancaster, New Hampshire (the "Subject Premises"), as of July 23, 2022. The subscriber T.D. is Isaiah Lafoe's mother.

Search Warrant of Subject Premises

28. On September 9, 2022, a U.S. Magistrate Judge in the District of New Hampshire issued a federal warrant authorizing the search of the Subject Premises in Lancaster, New Hampshire, the person of Isaiah Lafoe, and any electronic devices contained therein. FBI Special Agents and Task Force Officers executed the search warrant on September 14, 2022. Three electronic devices were seized during the search, including an Android phone, an Xbox gaming system and an Xbox Seagate external drive. The forensic review of those devices remains ongoing.

29. On September 14, 2022, LAFOE consented to a voluntary non-custodial interview. During the interview, LAFOE admitted that he lived at the Subject Premises and that he used the Target Phone -3620, Target Phone -2010, and Target Phone -7922 and used many different profiles on social media applications including Xbox, Google Duo, Snapchat, and TikTok, among others, on his phone. He also indicated that he had an Xbox gamertag and username of havokofdis98 and that he used a Snapchat account under username i_lafoe20, among others. He said that he met Victim-1 online and communicated with her in 2020 via phone and social media, and that he knew she was a minor under 14 years old when he communicated with her. When shown various images of child pornography retrieved from Victim-1's phone, Lafoe admitted that he received those

images and videos of child pornography from Victim-1 through social media and his phone, including on September 30, 2020, when he sent her a message saying, "Baby send me a pussy pic." Lafoe also stated that he and the victim would masturbate while on video chat and he would hit a button on the application to make an image of same.

30. Lafoe later provided a signed, written statement in which he stated the following in relevant part: "The next girl I messed with was named [Victim-1]. She initially lied to me when we first started talking on Monkey and told me she was eighteen. I could tell within a couple days that she was younger and she then admitted that she was thirteen. We then sent each other naked pictures and I asked her to send me certain naked pictures of her boobs or vagina and I asked her to send me videos of herself masturbating or touching herself." He further stated, "I did this with approximately eight other girls from the ages of thirteen to seventeen but I cannot remember anything about them." He also stated, "I know what I did was wrong as the girls I was involved with were too young for me. I sincerely regret my actions and hope that they and their families can forgive me and that I can get help."

31. On September 14, 2022, E.L., a relative of Lafoe, was interviewed by law enforcement and indicated that Isaiah Lafoe spends most of his time using dating apps or chat apps on his cell phone, to include Monkey, Snapchat, and WhatsApp. According to E.L., Lafoe is constantly talking to different girls and going from one relationship to another. Lafoe also frequently chats with people via Xbox chat feature, which E.L. had observed. E.L. was aware of Victim-1, a minor from New York who had heard Lafoe speaking with on the phone several times. According to E.L., Isaiah refers to Victim-1 as "baby" and "babygirl" but is now talking to another girl in Oklahoma. Lafoe has mentioned being romantically involved with minors under the age of 18 before and has mentioned having girlfriends aged 16 or 17 years old.

32. On September 14, 2022, T.D., Lafoe's mother, was interviewed by law enforcement and indicated that there was a recent issue with the Internet, so they changed the Wifi password in the Subject Premises. T.D. further explained that she had an application that monitors communications over the Xbox used by Lafoe and in early 2022, Isaiah Lafoe was caught sexually harassing girls over Xbox chat. T.D. stated that her husband had discovered this and had then taken the Xbox away. T.D. further stated that Isaiah has a "problem" and indicated that he sexually harasses underage girls over the Internet.

BACKGROUND ABOUT GOOGLE

33. Google is the provider of the Target Accounts, each an internet-based account identified by **lafoeisaiah28@gmail.com** and **miltonwilliamsaiesha@gmail.com**.

34. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

35. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

36. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

37. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

a. *Gmail*. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

b. *Contacts.* Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely,

unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

c. *Calendar.* Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar

d. *Messaging.* Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

e. *Drive and Keep*. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created

by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them.

f. *Photos.* Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves

files stored in Google Photos indefinitely, unless the user deletes them.

g. *Maps.* Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-byturn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

h. *Location History.* Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a

series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

i. *Google Pay.* A subsidiary of Google, Google Payment Corporation, provides Google Accounts an online payment service called Google Pay (previously Google Wallet), which stores credit cards, bank accounts, and gift cards for users and allows them to send or receive payments for both online and brick-andmortar purchases, including any purchases of Google services. Users may delete some data associated with Google Pay transactions from their profile, but Google Payment Corporation retains some records for regulatory purposes.

j. *Chrome and My Activity.* Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity. My

Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts in to automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

k. *Google Play.* Google Accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.

l. *Google Voice.* Google offers a service called Google Voice through which a Google

Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

m. *YouTube.* Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than one user can share control of a YouTube channel. YouTube may keep track of a user's searches, likes, comments, and change history to posted videos. YouTube also may keep limited records of the IP addresses used to access particular videos posted on the service. Users can also opt into a setting to track their YouTube Watch History. For accounts created before June 2020, YouTube Watch History is stored indefinitely, unless the user manually deletes it or sets it to auto-delete after three or eighteen months. For accounts created after June 2020, YouTube Watch History is stored for three years, unless the user manually deletes it or sets it to auto-delete after three or eighteen months.

38. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are

displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

39. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

40. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

41. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a

communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

42. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. Here, investigators believed that Isaiah Lafoe used the Target Accounts to communicate with Victim-1 (as well as potentially other victims), and the contents of those accounts will reveal whether Lafoe was using those accounts, and whether he was using those accounts to sexually exploit minors and/or coerce them into producing child pornography to send to him. Despite indicia from other sources suggesting that the accounts were owned and controlled by Lafoe, the exact identity of the user of the Target Accounts is unknown. The data sought here would therefore help establish the identity of who controlled the accounts when Lafoe was communicating with Victim-1.

43. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation. For example, in this case, Lafoe chatted and sent and received videos and images, including child pornography, with Victim-1 and any additional information about photos and emails sent or received by the user of the Target Accounts may provide information

about the communication of the offenses under investigation and which may be stored on Google servers.

44. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation. Here, the investigation concerns the production of child pornography by Isaiah Lafoe from a location in New Hampshire with at least one known victim in New York. The "user attribution" evidence contained in the Target Accounts would allow investigators to confirm the identity of the who used and controlled the account (including at the time Lafoe communicated with Victim-1), establish attribution as to the perpetrator(s) and Lafoe, and locate the location of Lafoe at the time that he received images and communicated with Victim-1 through the review of user content and GPS location information in the Target Accounts.

45. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.,* information indicating a plan

to commit a crime), or consciousness of guilt (*e.g.,* deleting account information in an effort to conceal evidence from law enforcement).

46. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. For example, apps for social media applications such as WhatsApp, Monkey, Omegle, or other dating apps such as Tinder might reveal information related to other methods of communication used by Lafoe to communicate with potential victims. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of persons who Lafoe may have distributed and received child pornography and instrumentalities of the crimes under investigation.

47. This investigation concerns the sexual exploitation of a minor and the receipt and production of child pornography sent by Isaiah Lafoe and the Target Accounts utilize various Google services. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users. In fact, even if subscribers provide Google with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

EXECUTION AT ANY TIME DAY OR NIGHT

48. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then

compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

CONCLUSION

49. Based on the forgoing, I request that the Court issue the proposed search warrant.

Attested to by the affiant:

Rebecca Gworek
Special Agent
Federal Bureau of Investigation

I, the Honorable Daniel J. Stewart, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on November 2, 2022 in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

Hon. Daniel J. Stewart
United States Magistrate Judge

ATTACHMENT A

Property To Be Searched

This warrant applies to information associated with the following Google accounts that are stored at premises owned, maintained, controlled, and/or operated by Google LLC, a company that accepts service of legal process and is headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043:

- **miltonwilliamsaiesha@gmail.com**
- **lafoeisaiah28@gmail.com**

ATTACHMENT B

Particular Things To Be Seized

I. Information To Be Disclosed By Google LLC ("Google" or "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for the account or identifier listed in Attachment A for the time period **September 1, 2020 to present**, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Target Account, including:

1. Names (including subscriber names, usernames, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;

5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers

6. Length of service (including start date and creation IP) and types of service utilized;

7. Means and source of payment (including any credit card or bank account number); and

8. Change history.

b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, usernames, source and destination IP address, name of accessed Google service, and all activity logs;

d. *Gmail.* The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails; as well as all forwarding or fetching accounts relating to the accounts.

e. *Contacts.* Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history.

f. *Calendar.* Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history

g. *Messaging.* The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.

h. *Google Drive and Keep.* The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, applications for any Android-user, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data and backups for any Android-user; SMS data and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record;

any location, device, other Google service (such as Google Classroom or Google Group), or third party application associated with each record; and all associated logs, including access logs and IP addresses, of each record.

i. *Photos.* The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses.

j. *Maps and Trips*. All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers Google - ISP List DOJ – CCIPS Last updated 8/6/20 7 receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history.

k. *Location History & Web & App Activity.* All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history

l. *Google Pay.* All payment and transaction data associated with the account, such as Google Pay and Google Wallet, including: records of purchases, money transfers, and all other transactions; address books; stored credit; gift and loyalty cards; associated payment cards, including any credit card or bank account number, PIN, associated bank, and other numbers; and all associated access and transaction logs, including IP address, time stamp, location data, and change history.

m. *Browsing, Search, and Application History.* All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.

n. *Google Play.* All activity relating to Google Play, including: downloaded, installed, purchased, used, and deleted applications, movies, music, television shows, books, magazines, and other files; details of the associated device and Android ID for each application, medium, or file; payment transactions; user settings; and all associated logs, including IP addresses, timestamps, and change history.

o. *Google Voice.* All Google Voice records associated with the account, including forwarding and other associated telephone numbers, connection records; call

detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including deleted voicemails; user settings; and all associated logs, including access logs, IP addresses, location data, timestamps, and change history.

p. *YouTube.*

1. Subscriber Information: Records associated with the account's YouTube registration, including the account's display name, IP logs, channel ID, account registration information, and registration email.
2. Contents: The contents of all media associated with the account on YouTube, whether active, deleted, or in draft, including: copies of videos and other media only if uploaded to, saved to, shared by or shared with the account; playlists; connected applications; associated URLs for each record; creation and change history; privacy settings for each record; and all associated logs, including IP addresses, locations, timestamps, and device identifiers;
3. Watch History: A record of the account's YouTube Watch History, including: accessed URLs and their associated duration, privacy settings, edits, comments, likes, chats, and other interactions, including associated URLs; search history; channels; subscriptions; subscribers, friends, and other contacts; IP addresses, change history, location information, and uploading account or identifier; the logs for each access by the account, including IP address, location, timestamp, and device identifier; and change history.

q. *Support.* All records of communications between Google and any person regarding the Target Account, including contacts with support services and records of actions taken.

r. *Complaints.* Information about any complaint, alert, or other indication of malware, fraud, or terms of service violation related to a Target Account or associated user(s), including any memoranda, correspondence, investigation files, or records of meetings or discussions about the Target Account or associated user(s) (but not including confidential communications with legal counsel).

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Information To Be Seized By The Government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of 18 U.S.C. §§ 2422(b) [Coercion and Enticement of a Minor], 2251(a) [Production of Child Pornography and Exploitation of a Minor], 2252A(a)(2) [Receipt of Child Pornography], 2252A(a)(5) [Possession of Child Pornography], and 1470 [Transfer of Obscene Material to a Minor], involving Isiah Lafoe, including for each Account or identifier listed on Attachment A, information pertaining to the following matters:

1. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s);
2. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the offenses under investigation and to the account owner(s);
3. Evidence indicating the owner of the account's state of mind as it relates to the crimes under investigation;
4. The identity of any person(s) who communicated with the account about the crimes under investigation, including the identity and whereabouts of co-conspirators, accomplices, and aiders and abettors in the commission of the criminal activity under investigation;
5. Records related to communications with any minor, including Victim-1 and Victim-2;
6. Records related to communications to persuade, induce, entice, or coerce any minor to engage in sexually explicit conduct;
7. Records related to the possession, receipt, or production of child pornography;
8. Records related to the location and identity of any victim of sexual exploitation of children;
9. Any child erotica or child pornography;

10. Any images of children, including photographs, drawings, sketches, fantasy writings, and notes showing an interest in unlawful sexual contact with children, and evidence assistance authorities in identifying any such children;
11. Internet history, including evidence of searches and visits to websites and applications that offer visual depictions of minors engaged in sexually explicit conduct or that offer a platform to communicate with others who are interested in unlawful sexual contact with children;
12. Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes, related to the coercion and enticement of minors;
13. Diaries, address books, notebooks, names, and contact lists of names and addresses of individuals (including minors).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.